The Discrete uniform Distribution is The Most Secure for Random Key Distributions

Philipp Harland

May 2025

Email: piranhafisherman@proton.me

Contents

1 Introduction **1**

2 Theorem **1**

1 Introduction

We can define the space of all keys as $K^\star$, where K is the set of letters the keys are assembled from.[1] *Here, $S^\star = \{(x_1, ..., x_n)|x_i \in S \forall i \in \{1...n\}\}$. Or, the set which is closed under f as a function of any 2 elements which are ordered tuplets with individual projections in S, where $f(a, b) = (\pi_1(a), ..., \pi_{dim\ a}(a), \pi_1(b)...\pi_{dim\ b}(b))$, which may be intuitively thought as the "side to side stack" of a and b, much like the concept of a direct sum in abstract algebra. Here, we let D_S denote a generic discrete distribution on S, i.e. a function that assigns a number in $[0, 1]$ to each element of S, and, $\sum_{s \in S} D_S(s) = 1$. This will be the case for the rest of the paper.*

2 Theorem

Let's say we have the space of all keys with constant length k, with their assigned probabilities – which we will denote as $(S^\star, D_S)$. The set itself will be defined as $\{(x, \prod_{i=1}^{k} D_S(\pi_i(x)))|x \in S^\star_{dim=k}\}$. If we and our adversary, A, have the exact same distribution used to generate keys in any given situation, we of course want to minimize any chance of our key being guessed and our message being revealed. The argument will be laid out as follows: (A) The probability of our adversary guessing our key is the product of the probabilities of the individual projections of

[1] Here, we consider a "key" a specific string which is used in a cryptosystem to encrypt another string.

our key. (B) The lower chance overall of our adversary guessing our key in any situation should be minimized. (C) If we slowly morph our given distribution into the uniform discrete distribution, we will see, over all distributions and all keys, that the adversary's chances get lower and lower. (Conc) Thus, the discrete uniform distribution is the most secure.
Additionally, this can also be argued for, given the fact any perturbation to the distribution would give our adversary an excess chance of guessing our key in a large set of situations.

This also works if we measure security in how much time our adversary would take on average to guess a given key over all keys, since the shapes of key distributions and computing time to guess an arbitrary key are very related. [2]

[2]This result has been stated in 2 other papers, but no formal/semiformal argument has been given in favor of the claim's veracity up until this point.